REMARKS

Claims 1-33 and 35-41 were presented and examined. In response to the Office Action, Claims 1 and 11 are amended, no claims are cancelled and no claims are added. Applicant respectfully requests reconsideration of pending claims in view of the above amendments and the following remarks.

I. Claims Rejected Under 35 U.S.C. §112

Claim 6 is rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. We respectfully traverse this rejection.

II. Double Patenting

Claims 1-3, 5-8, 11-14, 31-33, 35 and 41 are provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-29 of co-pending U.S. Patent Application Publication No. 2007/0223704 A1. Applicant holds in abeyance this rejection until such time as the claims on which the rejection is premised are granted.

III. Claims Rejected Under 35 U.S.C. §101

Claims 11-14 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. We respectfully traverse this rejection.

In response, Claim 11 is amended to recite a computer readable storage medium which is recognized as statutory subject matter. In view of Applicant's amendment to Claim 11, please reconsider and withdraw the §101 rejection of Claims 11-14.

IV. Claims Rejected Under 35 U.S.C. §103

Claims 1, 11 and 31 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 4,278,837 to Best ("Best"), U.S. Patent No. 6,278,782 to Ober, et al. ("Ober"), and U.S. Patent No. 7,181,620 to Hur ("Hur"). We respectfully traverse this rejection.

Claim 1 recites:

> 1. A method comprising:
> programming a **chip secret key** into a manufactured chip;
> sending the manufactured chip to a system original equipment manufacturer (OEM); and
> generating at least one **private** key for the manufactured **chip** in **response** to a received **key update request**, issued by the manufactured chip, if the received key **update request** is **authenticated**, to enable authentication of the manufactured chip **without disclosure** of the **private key** or **any unique device identification information** of the **manufactured chip**. (Emphasis added.)

While Applicant's argument here is directed to the cited combination of references, it is necessary to first consider their individual teachings, in order to ascertain what combination (if any) could be made from them.

Best is generally directed to a crypto-microprocessor chip that executes an enciphered program by piecemeal deciphering of enciphered instructions as needed. By deciphering small portions of the program only when they are needed, Best avoids any need for storing the program in deciphered form. (See col. 4, lines 41-46.) In contrast with Claim 1, Best does not disclose or suggest generating at least one private key for a manufactured chip in response to a received key update request if the received key update request is authenticated. Best discloses that the enciphering process of unit 184 is performed under the control of a secret cipher key, that is loaded into CMP 16 via line 163 by unit 184. (See col. 4, lines 60-65.) Nevertheless, loading of the key into CMP, for storage into register 5 and the removal of such lines prior to distribution of CMP to users, does not disclose or suggest the generation of at least one private key for a manufactured chip in response to a received key update request, much less if the received key update request is authenticated, as in Claim 1.

According to the Examiner, this feature of Claim 1, prior to amendment, is disclosed by Best at col. 14, lines 15-67. The passage referred to by the Examiner, however, describes operation of unit 184 for storing the key into CMP 116. In contrast with Claim 1, the passage referred to by the Examiner is directed to the explicit requirement that the storing of the key into the CMP is done at a different time and by a different operator than the storing of the enciphered program into memory 12. (See col. 14, lines 15-20.) Hence, neither this passage, nor any other portion of Best, either discloses or suggests generation of a private key in response to a received key update request, much less that private key generation is conditioned on authentication of the received key update request, as in Claim 1.

As correctly recognized by the Examiner, Best does not teach or suggest authentication of the received key update request, as in Claim 1. As a result, the Examiner cites Hur. We respectfully disagree with the Examiner's assertions and characterizations regarding Hur.

Hur generally relates to a cryptographic key distribution for network devices with minimal preconfiguration. As described by Hur, a first device, seeking secure communications with a second device, registers with a registration service to obtain a long-lived symmetric key. This key is used for registration with a key management service to receive a short-lived symmetric key. Hur teaches that the symmetric key is used to establish a session key for secure communication with the second device (see Abstract). According to the Examiner, authentication of the key request as in Claim 1 is disclosed by the Abstract, col. 6, lines 18-40, and col. 10, lines 33-38 of Hur. However, the passages referred to by the Examiner merely describe the use of a key management service to retrieve a short-lived symmetric key that is used to establish a session key for secure communication with a second device. We submit that the Examiner's citing of Hur fails to rectify the deficiency of Best in teaching or suggesting the combination of programming a chip secret key into a manufactured chip and generating at least one private key for the manufactured chip in response to a **received key update request** if the key update **request is authenticated,** as in Claim 1.

Furthermore, while Claim 1 is directed to programming a chip secret key into a manufactured chip and generating a private key for the manufactured chip in response to an authenticated key update request, Hur relates to devices with minimal preconfiguration, and not the manufactured chips, as in Claim 1. Moreover, neither Best nor Hur describes a combination of programming a chip secret key into a manufactured chip and generating at least one private key for the manufactured chip in response to an authenticated received key update request, as in Claim 1. The Examiner's reliance on Best to disclose a combination of programming a chip secret key into a manufactured chip and generating at least one private key for the manufactured chip in response to a received key update request is improper. Best does not provide both programming of a chip secret key into a manufactured chip, and generating at least one private key for the manufactured chip in response to a received key update request, since the portions of Best referred to by the Examiner are limited to the storage of a key into CMP 116, by generating a random number for use as a key. Hence, no combination of Best in view of Hur can teach or suggest the combination of programming a chip secret key into a manufactured chip and generating at least one private key for the manufactured chip in response to a key update request, if the received key update request is authenticated, as in Claim 1.

As correctly recognized by the Examiner, the combination of Best and Hur does not teach when the update request is made by the chip. As a result, the Examiner cites Ober. Ober relates to a method of implementing a key recovery system. As described by Ober, a Diffie-Hellman public key method, which is preferred over elliptic curve in RSA, is used for generating a recovery key encryption key (RKEK) because each party contributes equally to the generation of the RKEK and no party has an advantage over the over. (See col. 3, lines 15-21.) Nevertheless, because Ober relies on public key/private key ecryptography, the disclosure of the public key assigned to the chip would provide unique device identification of the chip during subsequent authentication.

Conversely, as recited by amended Claim 1, the at least one private key is generated for the manufactured chip in response to received key update request, issued by the manufactured chip, if the received key update request is authenticated, to enable authentication of the manufactured chip without disclosure of the private key or any unique device identification information of the manufactured chip. Since Ober is preferably limited to the Diffie-Hellman public key method, the public key of a chip would provide unique device identification of the chip during an authentication process. As a result, it is improper for the Examiner to rely on Ober since it cannot be said that Ober generates at least one private key for a manufactured chip to enable authentication of the manufactured chip without disclosure of the private key or any unique device identification information of the chip, as in Claim 1.

Therefore, the Examiner has failed to identify, and Applicants are unable to discern any portion of Best in view of Ober and further in view of Hur or the references of record, that discloses, teaches, or suggests the combination of programming a chip secret key into a manufactured chip and generating at least one private key for the manufactured chip in response to a received key update request if the received key update request is authenticated, to enable authentication of the manufactured chip without disclosure of the private key or any unique device identification information of the manufactured chip, as in Claim 1.

For each of the above reasons, Claim 1 and all claims which depend from Claim 1 are patentable over Best in view of Ober and further in view of Hur, as well as the references of record. Therefore, please reconsider and withdraw the §103(a) rejection of Claim 1.

Each of the Applicant's other independent claims, and each claim which depend from those claims are patentable over the cited art for similar reasons. Therefore, please reconsider and withdraw the §103(a) rejection of Claims 11 and 31.

DEPENDENT CLAIMS

In view of the above remarks, a specific discussion of the dependent claims is considered to be unnecessary. Therefore, Applicants' silence regarding any dependent claim is not to be interpreted as agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending (1) are in proper form, (2) are neither obvious nor anticipated by the relied upon art of record, and (3) are in condition for allowance. A Notice of Allowance is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: October 15, 2009

By: ______________________
Joseph Lutz, Reg. No. 43,765

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Telephone (310) 207-3800
Facsimile (408) 720-8383

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web to the United States Patent and Trademark Office on October 15, 2009.

____
Si Vuong